29.01.03.H0.10 Incident Management

Approved: April, 2014
Next Scheduled Review: April, 2019

Procedure Statement

The number of computer security incidents and the resulting cost of business disruption and service restoration continues to escalate. Implementing solid security policies, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents, are some of the actions that can be taken to reduce the risk and drive down the cost of security incidents.

Reason for Procedure

This procedure provides a set of measures that will mitigate information security risks associated with incident management and describes the requirements for dealing with computer security incidents. It applies to all individuals who use Texas A&M University-Texarkana (TAMUT) Information Resources.

Definitions

CIA triad: Confidentiality, Integrity and Availability.

Incident Response Team (IRT): Personnel responsible for coordinating the response to computer security incidents in an organization. The IRT holds regular meetings to review any incidents that have occurred, and discusses projects relating to IT Security. Emergency meetings may also be called at the discretion of the CIO or ISO if an incident needs immediate attention. The team members and their roles include:

Information Security Officer: Advises team of incidents that have occurred and updates members on security projects.

FERPA Officer: Advises team of all aspects regarding FERPA, as well as enrollment management processes.

PCI Compliance Representative: Advises team regarding PCI Compliance, as well as Business and Finance processes.

Financial Services: Advises team of all financial operations for students.

Academic Affairs: Advises team regarding the processes within Academic Affairs.

Risk Management & Compliance: Advises team of risk and compliance matters.

Judicial Affairs: Advises team of student judicial affairs.

UPD Representative: Advises team of any criminal computer incidents.

Information Resources (IR): Any computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing websites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, tablets, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), smartphones, telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it includes the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Information Resources Manager (IRM): Person responsible to the State of Texas for management of the agency's information resources. The designation of an agency information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the agency's information activities, and ensure greater visibility of such activities within and between State agencies. The IRM has been given the authority and the accountability by the State of Texas to implement security policies, procedures, practice standards and guidelines to protect the Information Resources of the agency. At TAMUT, the IRM is the CIO.

Information Security Officer (ISO): Person responsible to the executive management for administering the information security function within the University. The ISO is TAMUT's internal and external point of contact for all information security matters.

Security Incident: Assessed event of attempted entry, unauthorized entry, or an information attack on an automated information system. It includes unauthorized probing and browsing, disruption or denial of service, altered or destroyed input, processing, storage, or output of information, or changes to information system hardware, firmware, or software characteristics with or without the users' knowledge, instruction, or intent.

Procedures and Responsibilities

1. HOW TO REPORT AN INFORMATION SECURITY INCIDENT

TAMUT's ISO is required to establish and follow Incident Management Procedures to ensure that each incident is reported, documented and resolved in a manner that restores operations quickly and if required, maintain evidence for further disciplinary, legal, or law enforcement actions.

1.1 Incidents involving computer security will be managed by TAMUT's ISO and will be reported as required by federal or state law or regulation.

1.2 All faculty members, staff and/or students must promptly report any unauthorized or inappropriate disclosure of confidential information.

1.3 Additional information on Information Classification is described in TAMUT's 29.01.03.H0.31 Information Classification Procedure.

1.4 There are two ways to report an incident:

1.4.1 E-mail: itsecurity@TAMUT.edu

1.4.2 Call: 903-886-5425

2. INCIDENT CATEGORIES:

2.1 **Level 1** – These are the least severe and most common types of incidents. They have no widespread effect on any TAMUT function. Level 1 incidents will be handled by the IT department via work order. Incident types and quantities will be tracked and reported. Incident reports will be sent to the Department of Information Resources (DIR) via their Security Incident Reporting System (SIRS).

2.2 **Level 2** - Incidents that have a small impact on operational functionality but have no impact on the overall business function of the University. Level 2 incidents will be handled by the IT department via work order and will be reported to the CIO or ISO. IT personnel will continue to monitor the incident after remediation and will report findings to the CIO and ISO for as long as they deem necessary. Incident types and quantities will be tracked and reported. Incident reports will be sent to the Department of Information Resources (DIR) via their Security Incident Reporting System (SIRS).

2.3 **Level 3** - These are the most severe incidents. They have a major impact on either business or operational functions at TAMUT and may prevent the University from fulfilling its mission. This category also includes incidents that may cause reputation or financial damage to TAMUT. Level 3 incidents are considered an emergency and will considered a top priority. The incident will be handled by the IT department via work order, and all steps taken must be approved by either the CIO or ISO. IT personnel will continue to monitor the incident after the threat has been mitigated, and must report all findings to the CIO and ISO for as long as they deem necessary. An incident report will be prepared by the ISO for review by the CIO, the Administrative Council. Incident types and quantities will be tracked and reported to the Department of Information Resources (DIR) via their Security Incident Reporting System (SIRS). The following are examples of the categories of IT security related incidents:

Incident Categories	Description	Examples
Level 1	No widespread effect on TAMUT functions	• Minor rule violations by an employee • Detection and removal of viruses or malware
Level 2	No impact on overall business functions, but do have an impact on operational functions	• Repeated reconnaissance activity from the same source • Attack blocked by TAMUT's security infrastructure • Regular occurrences of Level 1 incidents • Successive attempts to gain unauthorized access to a system
Level 3	Complete loss of critical business function related to database or operating system	• Server unresponsive • Environment out of disk space

Related Statutes, Policies, or Requirements

Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C, Rule § 202.75, Information Resources Security Safeguards

References

Copyright Act of 1976
Foreign Corrupt Practices Act of 1977
Computer Fraud and Abuse Act of 1986
Computer Security Act of 1987
The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
The State of Texas Information Act
Texas Government Code, Section 441
Texas Administrative Code, Chapter 202
IRM Act, 2054.075(b)
The State of Texas Penal Code, Chapters 33 and 33A
DIR Practices for Protecting Information Resources Assets
DIR Standards Review and Recommendations Publications

Contact Office

Information Security Officer, 903-886-5425